Elections Division of
Colorado Secretary of State's Office

Colorado Election Fact Sheet

Protection of Voting Systems Overview

---

1) Introduction

Colorado elections are among the most secure in the nation, and the 2020 presidential election was the most secure election to date. The Secretary of State's Office and the State of Colorado spent years, spanning several administrations—led by secretaries from both major political parties—working to increase election security through statutory changes, rule updates, and process innovations. As a result, Colorado has a secure, transparent, and resilient election model, which is highly respected around the country.

2) Protection of Voting Systems

a) Initial testing, certification, and use authorization. Colorado law prohibits county clerks from using any voting system until it is first tested, certified, and approved for use in Colorado by the Secretary of State's Office.[1] This process ensures that all voting systems in Colorado satisfy 938 standards and requirements under both federal and state law.[2] The certification process requires voting systems providers deliver to the Secretary of State's Office a technical data package and a proposed test plan that addresses all of the requirements.[3] Career staff at the Secretary of State's office independently review the provider's technical data package and proposed test plan to ensure it covers the applicable specifications and requirements. After the Secretary of State's Office approves the test plan, a federally accredited Voting Systems Test Lab executes the approved test plan by testing the system's functional compliance with each of the stated requirements, and performs an application penetration test to identify potential undisclosed vulnerabilities, and a source code evaluation.[4] (See Secretary of State's Office Certified Systems page.) When the testing is complete, the Voting Systems Test Lab provides a final test report and

[1] C.R.S. Title 1, Article 5, parts 5-7; 8 C.C.R. 1505-1 § 21
[2] C.R.S. Title 1, Article 5 parts 5-7; 8 C.C.R. 1505-1 § 21
[3] 8 C.C.C. 1505-1 § 21.2
[4] 52 USC § 20971

{Published Oct. 22, 2021}

a completed requirements matrix, and Secretary of State career staff evaluate the test report and other system documentation to identify additional testing that may be needed before recommending certification. The Secretary of State then reviews the work and recommendations of career staff and, if satisfied, certifies the voting system for use in Colorado. Any significant upgrade or change to a certified voting system must undergo the same testing regimen.

b) Trusted build and documented chain-of-custody. After a voting system is certified, the Voting Systems Test Lab securely delivers to career staff the exact software that was successfully tested and certified, along with the hash value of the software code. Career staff independently verify that the software received by the test lab has the same hash values, and then compile that software so that it can be installed on the various components of the system. The software code is secured in a restricted-access safe, where it remains unless removed to install the system software at counties that use the voting system.

Only career staff of the Secretary of State's Office install the certified version of the software on the voting system's hardware components,[5] usually onsite at each county that uses the system. This process is known as "trusted build," and ensures that every voting system component in Colorado is running only the software that was successfully tested by the test lab and authorized for use in Colorado by the Secretary of State.

Immediately after installation of trusted build, the county election officials affix tamper-evident seals to specific locations of the voting system's hardware components. Each seal has a serial number, and county election staff record the serial numbers of all seals on a chain-of-custody log for each device, together with their names and signatures, and the date and time of trusted build. Then, each time the county uses a particular device during an election or for training purposes, at least two staff members or citizen election judges of different party affiliations must complete another chain-of-custody log entry, verifying the numbers and locations of every seal affixed to the device. Because the seals would need to be removed or disturbed in order to install any other program on the component after trusted build, the fact that they remain intact before and after each use of the component helps provide evidence that no one tampered with the device. If chain-of-custody for a particular device is incomplete or "broken," the county must notify the Secretary of State's Office and may not use the device until the Secretary of State Office's career staff re-installs trusted build with the program that was successfully tested and certified.[6] (See Secretary of State Office's Voting Systems Trusted Build Procedures.) Additionally, Secretary of State's Office career staff issue mandatory "Conditions of Use" for certified voting systems to further increase the security and integrity of Colorado's certified voting systems.[7] The Conditions of Use are reviewed with each new certification of a voting system, and updated if necessary.

c) Pre-election testing. The next safeguard – pre-election testing – ensures that each county's voting system is properly configured and programmed for each election in which the voting

[5] 8 C.C.R 1505-1 §§ 1.1.42, 20, 21

[6] 8 C.C.R 1505-1 § 21

[7] C.R.S. 1-5-608.5(3)(b)

system is used. Colorado law requires county clerks to conduct two voting systems tests before each election.

First, the county clerk must conduct a hardware and diagnostic test on every voting systems component that will or may be used in the upcoming election. The hardware and diagnostic test ensures that each device operates, outputs, and functions correctly before deployment for use in an actual election.

Second, the county clerk must convene a bipartisan testing board (the members of which are appointed by the county chairpersons of the major political parties) and conduct a pre-election logic and accuracy test on randomly selected voting systems components. The purpose of the logic and accuracy test is to verify the voting system is properly configured and programmed to accurately tabulate votes. For example, races for statewide offices permit voters to vote for one candidate in each race, while many local races permit voters to vote for two or more candidates. The county clerk and bipartisan testing board must verify the voting system was set up correctly by marking, scanning, and then verifying by hand the voting system's tabulation of test ballots. The logic and accuracy test verifies that the system correctly records all valid votes, under votes, over votes, and blank votes.

In Colorado, each county's logic and accuracy test is open to the public, and must be conducted at least 21 days before the election. Following the logic and accuracy test, the county may not change the set-up of any tabulation device before the election.[8] If any change to the election database must occur because of problems identified during or after the LAT, the same testing board must conduct another LAT on that piece of equipment before the election.[9]

d) Post-election auditing. After each election and before any results are officially certified, Colorado conducts a statewide bipartisan risk-limiting audit (RLA). Please see the risk-limiting audit fact sheet for more information about Colorado's first-in-nation bipartisan risk-limiting audits.

e) Other protections. Voting system are prohibited from being connected to the internet.[10] Bipartisan teams of election judges or county staff maintain documented chain-of-custody of every voting device after trusted build.[11] Passwords for voting systems are regularly changed and are required to be sufficiently complex.[12] Voting system providers are not granted administrative or user access to a county's election management system. Career staff at the Secretary of State's Office conduct onsite security audits in randomly selected counties to verify compliance with these important security protocols.[13]

[8] 8 C.C.R. 1505-1 § 11.3.2
[9] 8 C.C.R. 1505-1 §§ 11.3.2(e)(1-5)
[10] 8 C.C.R. 1505-1 §§ 20.6, 20.8, 21.4.10 (d)(3)
[11] 8 C.C.R. 1505-1 §§ 20.4, 20.10.1
[12] 8 C.C.R. 1505-1 § 20.6.1
[13] 8 C.C.R. 1505-1 § 20.3.1